IDENTITY VERIFICATION METHOD USING A CENTRAL BIOMETRIC AUTHORITY

Field of the Invention

The present invention relates to an identity verification system; and, more particularly, to a method for effectively establishing the identification of users by utilizing a central biometric authority (CBA).

Background of the Invention

It is known that a public/private key infrastructure (PKI) is an excellent mechanism to ensure that data remains confidential and unchanged during transit over insecure networks such as the Internet. The PKI is based on the premise that a user has two mathematically related numerical keys, a private key and a public key, which serve to encrypt data. It is possible to secure a message by encrypting it with a sender's private key and a receiver's public key, which is obtained from a repository known as a certificate authority (CA). The receiver can read the message by decrypting it using his private key and the sender's public key.

The keys used in the PKI are very long; and, the longer they are, the more secure the system is. It is not feasible,

however, for a user to remember or input a long key, e.g., 64 character or longer, when the user wants to send or receive a message. To prevent unauthorized users from accessing private keys and thus falsely originating, reading or changing messages, private keys are usually protected by a secret code.

Secret codes such as a personal identification number (PIN) and a password can be compromised through the use of various techniques well known in the art. For instance, people often choose easy to remember pins and passwords, which also make them easy to guess. Birthdays, children's names and social security numbers are among the most commonly chosen. To combat this, many organizations require that passwords be changed often, and many PINs are assigned to prevent easily guessed PINs. Unfortunately, many times this leads to people writing down the secret information, making it accessible to fraud perpetrators.

Shoulder surfing is also a known technique that can be used to compromise secret codes. This simply involves a fraud perpetrator watching over the shoulder of the person entering the code as a secret code is entered.

Also brute force attacks can compromise secret codes. This method simply involves rapidly entering many codes, until the secret one is stumbled upon. Long codes, mixing letters and numbers and frequent changing of codes can

prevent the success of brute force attempts. Additionally, systems locking up after a predefined number of incorrect password attempts can prevent the success of brute force attacks.

If the private key is compromised by one of the various techniques, then it is no longer possible to ensure that information is kept confidential and unchanged. Therefore, the reliability of the PKI depends on any method used to secure the private key.

Various techniques have been suggested to enhance the performance of the PKI, such as securing the private key with biometrics instead of secret codes. Biometrics are more secure than secret codes; and therefore the security of the PKI can be enhanced. Biometrics are technologies that verify identity based upon one's physiological or behavioral characteristics, such as one's fingerprint, eye scan, voice print, hand geometry, facial image or signature. Biometrics can verify one's identity by either performing a one-to-one comparison to authenticate a submission or by performing a one-to-many comparison to identify one's submission out of a database containing a plurality of biometrics samples. A biometric sample is either the direct information obtained from the user, e.g., fingerprint, hand image, voice print,

facial image, handwriting sample or facial image, or processed form of such information. For example, a biometric sample includes one's fingerprint and a minutia template based on one's fingerprint. By securing the private key with a biometric, the sender can assure the integrity of the private key so that a message using it will not be fraudulently originated. Likewise, a receiver protecting his private key with a biometric can rest assured that no one will be able to read the message that is intended for his eyes only. Only after a local verification of the biometric submission releases a local private key, the message can be originated or read.

However, even with a biometrically protected private key, neither party is assured that biometric authentication is processed on the other end. That is, the sender is not assured that the intended receiver is reading the message and the receiver is not assured that the intended sender sent the message. For example, neither party is assured that the other party uses a biometric, instead of a secrete code to protect the private key. There are myriad problems with one party relying on the other to use a biometric system to secure the private key. Neither party can be certain that other party has installed a biometric system on its computer; nor can they be certain that the other party's private key is

securely protected by the biometric.

Furthermore, there is no quality control over enrollment. That is, there is no way to ensure that samples submitted during enrollment belong to a claimed enrollee. And a fake sample could have been enrolled. Additionally, neither party has any control over the environment of other party's computer. In other words, there could be a network of supercomputers working to hack into the biometrically protected key. Dozens of attempts might be made before a sample is falsely verified.

If the sender and the receiver know with certainty that the other's private keys are being secured with a biometric, and if they could receive, interpret and rely on a biometric verification score, then the process would be secure. In addition, there are different disciplines of biometrics (e.g., voice verification, finger scanning, iris scanning, retina scanning, hand geometry), and many vendors within each of these disciplines, each having its own accuracy levels. There is currently no infrastructure for interpreting the verification score of each of these vendors. As such, if the receiver learns that the sender is verified on a biometric system from a vendor with a score of 75, they would have difficulty in determining if this was a good match. Finally, there is no way for a sender or receiver to ensure that the results of a biometric comparison are in fact legitimate.

Because in the conventional approach all biometric verifications are performed on local machines, there is no assurance that the biometric verification is processed as it should.

A revocation list used in the PKI is a list of certificates that have been compromised and are thus no longer valid. The fundamental problem with relying solely on this list to confirm that a certificate is being used by a legitimate user is that revocation lists are not immediately updated. The moment a private key is compromised it does not appear on the revocation list. No one, with the exception of the fraud perpetrator, knows that a compromise has taken place and certainly he or she will not notify the CA to add that certificate to the revocation list. In addition, once the certificate is reported as compromised, there is a time lag before the distributed lists are updated. The real value of a revocation list is to prevent repeated fraud to be perpetrated on the same certificate.

Without the CBA infrastructure, individual institutions will have to maintain local databases of biometric enrollments. There are a number of problems with this scenario. First, there is a large overhead for a typical company to create and maintain a biometric enrollment for each customer. This includes the cost and time to properly identify each enrollee, train each enrollee on proper system

use, etc. Second, customers may trust a company enough to buy from them, but may not want to enroll in their biometric system. Third, there are a number of bills pending relating to the use of such local databases. Companies risk losing the right to use their database in the manner they intend, or having a databases or related processes that do not comply with new laws. There could be substantial overhead in restructuring databases to comply with new laws. There are liability issues with maintaining databases of enrollments. It is preferable for companies avoid such risks and not maintain an internal biometric database.

Summary of the Invention

It is, therefore, a primary object of the present invention to provide a method capable of improving the performance of an identity verification system by verifying the identification of users using a CBA.

In accordance with one aspect of the present invention, there is provided a method for verifying the identity of one or more parties that are transmitting information, comprising the steps of:

(a) generating, on the sender side, a first message to the receiver, wherein the first message includes a substantive message to be transmitted and a unique message identifier

(UMI);

(b) issuing, by one the parties, a second message concerning a posting to a central biometric authority (CBA), wherein the second message includes a biometric sample of the party, and the UMI, and a submission profile of the party;

(c) providing, at the CBA, verification of the party's biometric sample; and

(d) issuing, by the CBA, a third message including a verification result of the party.

In accordance with another aspect of the present invention, there is provided A method for verifying the identity of one or more parties to a transaction using biometrics whereby a third party stores the biometric templates and performs the identity verification.

Brief Description of the Drawings

The above and other objects and features of the present invention will become apparent from the following description of preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 is a schematic block diagram of an identity verification system in accordance with the present invention; and

Figs. 2A-2D present drawings for illustrating implementations of a CBA in accordance with the present invention, respectively.

Detailed Description of the Preferred Embodiments

Referring to Fig. 1, there is provided a schematical block diagram of an identity verification system 100 incorporating therein a method for performing biometric verifications to authenticate the identification of users in accordance with the present invention.

A unique message identifier (UMI) block 110 establishes the identity of two parties that are involved with a message or transaction. The UMI block 110 has a sender/authorized transactor (AT) ID, a receiver/proxy ID, a data and time stamp and a hash value. The hash value is used to ensure that the message/biometric has not been altered. An additional number may be added to ensure that the UMI block 110 is indeed unique.

A submission profile record block 120 describes to the CBA 140 the system that captured a biometric template. The block 120 has information on a hardware maker and model, a software maker and version number, and which sample is being submitted.

A verification requirement record block 130 tells the

CBA 140 the criteria that the sender/AT sets out for the receiver/proxy to successfully verify. The block 130 has a verification score being required to verify and a maximum number of attempts being allowed to attain the verification score and a minimum ESL, as defined below.

The CBA 140 has various features as follows. First of all, an ideal candidate company to serve as the CBA 140 is a trusted independent third party with the transaction processing capability to handle a high throughput of submitted samples, perform verification on the samples, and provide verification scores. These characteristics are similar to that of a CA (Certificate Authority). As such, there is likely to be much synergy from the CA and the CBA being the same entity. In the CBA 140, the enrollment process involves identifying an enrollee and collecting biometrics samples. The robustness of the identification process that performs during the enrollment will dictate to what degree the enrollment can be relied upon. This robustness is qualified by an enrollment security level (ESL). Whenever a verification score is reported, the ESL of the template to which comparison is being made is also returned.

In a preferred embodiment of the invention, it is likely that the CBA 140 will accept enrollments from other parties. Financial service providers are likely to serve

among enrollment locations. During account opening, identification of customers already takes place, and therefore it would be a suitable time to enroll a new user into the CBA 140. The ESL will be affected by the trustworthiness of the point of enrollment. Thus, an enrollment at a large bank would have a much higher ESL than a self-guided enrollment at home.

In a preferred embodiment of the invention, it is likely that a single user will have multiple enrollment templates on file at the CBA 140. These enrollments may include enrollments from vendors of the same technology discipline, enrollments from different disciplines, enrollments of different biometric samples, enrollments with different ESL's, and any combination of the above. The actual number of enrollments for a given individual depends on their identification needs.

In addition to the templates, additional information or pointers to information can be maintained in the enrollee information profile (EIP). This information can only be released by the permission of the enrollee, and for specific purposes. For instance, the enrollee's age may be released to gain access to a bar or to purchase alcohol or cigarettes.

The enrollee's credit rating information may be

released when applying for a new credit card or mortgage. Enrollee's group, group permissions, and organization affiliations may also described in the EIP. This would allow, for instance, a hotel operator to determine if someone is eligible for a corporate rate based upon the persons group or company affiliations.

It is possible for the enrollee to designate certain portions of his EIP as "open" to certain people or groups. This means that no submission from the enrollee is needed to access this information. For instance, an enrollee might make a list of his allergies to medicines open to anyone who is a member of the emergency room doctor group.

When a user enrolls into the CBA 140, the biometric template is stored in the CBA 140. Instead of multiple organizations (every organization that a customer does business with) having biometric enrollments and processing each submission, this activity is limited to the trusted CBA 140. Biometric submissions are never shared with anyone besides the CBA 140. The two parties communicating with each other never share submissions with one another. Biometric information shared between the parties is limited to verification scores and ratings, which are shared only via the CBA 140. The enrollment templates on file with the CBA 140 are never released during standard transactions. The structure is analogous to the secure electronic transaction (SET) protocol

for credit card transactions. In the SET framework, a merchant never sees the credit card number of a customer, only the approval that the credit card is valid and sufficient credit is available. In the same way, with CBA, biometric submissions are never shared between parties, only the approval that verification took place is shared.

It is also possible for an enrollee to designate another person or persons as a proxy for themselves. This may be a full function proxy, or limited to specific transactions. A permanent proxy authorization posting is made, which grants the permissions. Such proxies, in most cases, can be revoked. By definition, the CBA 140 is a central authority, acting as a simple entity. While the CBA 140 virtually acts as a single authority, where verification can be performed and scores returned the physical structure may be distributed. This distribution may be for performance, throughput or other reasons. Different groups offering competing CBA services may duplicate each other services and data. There may be duplicate (in whole or part) CBAs for backup purposes, e.g., disaster recovery.

For off-line transactions, biometrics templates will be stored on portable medium such as smart cards or magnetic stripe cards. There is a need, however, to allow for easy recreation of these cards should they be lost or stolen. The CBA serves as a repository for these templates. As such,

there may be templates on record for an enrollee that are not accessible on a normal day to day basis, but are only accessible by certain organizations to recreate lost templates. For those companies that do maintain local biometrics databases, the CBA will serve as an off site back up/hot site facility for the templates in case of data loss or system failure.

The need for a notary public is to establish the one's identity. Such identity is currently established by relying on one's photo ID and signature. In cases where a biometric can be submitted, the service by a notary public is accomplished by the CBA 140 more effectively.

After collecting a biometric sample, features are extracted to create the biometric data (sometimes referred to a template). The term "biometric sample" includes the direct sample and the template created therefrom. The CBA 140 architecture can function with either the biometric sample or the measurements of the sample. There are advantages and disadvantages of each. By sending the measurements of the sample, less information needs to be sent, thus requiring less transaction time and less bandwidth. By sending the entire sample, less processing power and time is required at the point of capture, and more updated extraction algorithms can be used at the CBA 140. In addition, if the entire

sample is sent, the sample can be more processed through multiple systems from different vendors.

Verification scores are only valuable if the reader of the score knows how to interpret it. Unfortunately, each biometric vendor reports scores in different ways. In some cases the scale is a logarithmic 0 to 1, in other cases the scale is a linear 1 to 100. In some cases, high scores are best, and in other low scores are best. Even when the same relative scales are used, different technologies and different vendors have different accuracy levels. Thus, a score of 75 out of an ideal 100 on a retina scan unit may carry a very different confidence level than a 75 out of an ideal 100 on a dynamic signature verification system. As such, the verification score-rating table classifies vendors output into easily understandable categories. The objective analysis relates to the different vendors on the same scale, and the subjective analysis relates to different technologies based on their underlying performance. This analysis classifies each verification score into categories (or rating) such as "high", "medium", "low", and "fail" with regard to the confidence of the match. This latter analysis is optional, and not a required aspect of the CBA 140.

Hereinafter, four embodiments of the CBA 140 will be illustratively provided in detail with reference to Figs. 2A-2D, which depict the embodiments, respectively. The first

and second embodiments relate to electronic commerce and messaging and the third and fourth embodiments relate to face to face transactions.

Specifically, in a first embodiment of the present invention, a method to verify the identity only of the sender of a message is described. A sample transaction is a customer sending a message to their bank to wire transfer money into their stockbroker's account.

With reference to Fig. 2A, at step 11, a sender generates a message to a receiver. The message includes the substantive message? and the UMI.

Meanwhile, at step 12, the sender generates a message relating to a posting to the CBA. This message includes the sender's biometrics sample, the UMI, and the sender's submission profile record. At step 13, it is necessary to take place only if the receiver desires verification of the sender's identity. In many cases (low risk level involved with message communication, low chance of suspected fraud, junk e-mail, etc.) this verification may not be desired, and the CBA process may never be completed. In this case, the step 12 will remain "unclaimed". An aging off to expiration scheme can be implemented to remove unclaimed posting after a predetermined amount of time. Note that in actual implementation, process at the receiver side may automate a seamless verification of every message regardless of content.

Receiver generates a message relating to a receiver posting to the CBA, the message including only the UMI, as received from the sender's message. At step 14, the CBA generates a reply to a receiver's posting including only the sender's verification results.

With reference to Fig. 2B, the second embodiment of the invention is provided, wherein a method to verify the identity of both the sender and the receiver of a message is described. A sample transaction is someone sending a secure message to an important client. To accomplish this, a synchronous or secret key is created for the transaction by the sender, and held from the receiver until they have been biometrically identified to the satisfaction of the sender.

Specifically, at step 21, a sender generates a message to a receiver. The message includes the substantive message encrypted with a synchronous key and the UMI.

Meanwhile, at step 22, the sender generates a message relating to a posting to the CBA. This message includes the sender's biometrics sample, the UMI, the sender's submission profile record, the synchronous key used in step, and the verification requirements record. At step 23, the receiver generates a message relating to a receiver posting to the CBA including the UMI, as received from the sender's message and the receiver's biometric sample. At step 24, the CBA

generates a reply to the receiver's posting to CBA including the sender's verification results and the synchronous key to decrypt the message.

Referring now to Fig. 2C, the third embodiment of the invention is given, wherein a method to verify the identity of a person presenting themselves to complete any face-to-face transaction (authorized transactor or AT). A sample transaction is a credit card transaction at point of sale, a cash withdrawal at an ATM or teller window, or someone picking up their car at the mechanics shop.

Specifically, at step 31, at a point of transaction (POT) the POT operator (e.g., cashier) issues a message relating to a POT posting to CBA. This message includes the authorized transactor (AT)'s claimed identity, the AT's biometric sample and the POT submission profile record. At step 32, the CBA compares the biometric sample from the step 31 to that registered on the AT and generates the reply to the POT posting. This message includes only the AT's verification score/rating.

Referring to Fig. 2D, the fourth embodiment of the invention is provided, wherein a method to verify the identity of someone who is standing in as a proxy for an authorized transactor is illustrated. A sample transaction includes a proxy going to a day care center to pick up an AT's child. Specifically, at step 41, the AT generates a

message relating to a proxy authorization posting, including their biometric sample, the UMI, the submission profile record, an instruction block and the verification requirements record. The instruction block is a message to the POT operator as to what the proxy should be allowed to do on their behalf. The instruction block will usually contain expiration data in addition to the allowed actions. At step 42, the POT operator generates a message relating to a POT posting to the CBA, including the proxy's claimed ID, the proxy's biometrics sample, and the POT submission profile record. At step 43, the CBA generates a reply to the POT posting, which includes the AT's name and verification results and the instruction block.

As may be seen from the above, by centralizing the verification of the sender's and/or receiver's biometrics sample, each can be assured as to the other's identity. Since there is control over the enrollment and verification conditions at the CBA, verification can safely be interpreted as an assurance of identity. In addition, since a message specific key as well as the PKI private keys is used, the concerns of non-biometrically protected copies of private keys are mitigated. Finally, by using conversion tables, users of different biometric systems can set minimum verification thresholds for users of systems different from their own. While it is not essential for a CBA system to be

used in conjunction with a PKI, all embodiments of the present invention to be described later use a CBA in addition to a PKI. It is recognized that, although PKI and CBA work very well together, they may be used independently.

Prior to the CBA, there has been little work to establish an infrastructure to automate the exchange of biometric samples for day to day identification needs. The CBA serves as a point of verification for any transaction where identity must be established. Additionally, an authorized transactor can designate another person as their proxy to carry out a transaction. Furthermore, the need for each company to build and maintain local databases of biometric enrollments and process verifications are reduced. And since biometrics samples and templates are not shared with anyone except the trusted CBA, privacy is increased. Finally, there is an ability to determine the authority of an individual to perform a specific transaction, by consulting the enrollee information profile.

While the present invention has been shown and described with respect to the particular embodiments, it will be apparent to those skilled in the art that many changes and modifications may be made without departing from the spirit and scope of the invention as defined in the appended claims.